PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/08, 9/16, 9/30

A1

(11) International Publication Number: **WO 99/09700**

(43) International Publication Date: 25 February 1999 (25.02.99)

(21) International Application Number: PCT/IL98/00381

(22) International Filing Date: 13 August 1998 (13.08.98)

(30) Priority Data:
121551 14 August 1997 (14.08.97) IL

(71)(72) Applicant and Inventor: BARKAN, Mordhai [IL/IL]; Brande Street 24, 49600 Petah Tikva (IL).

(74) Agent: ZUTA, Mark; Ben Yehuda Street 19, 49373 Petah Tikva (IL).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

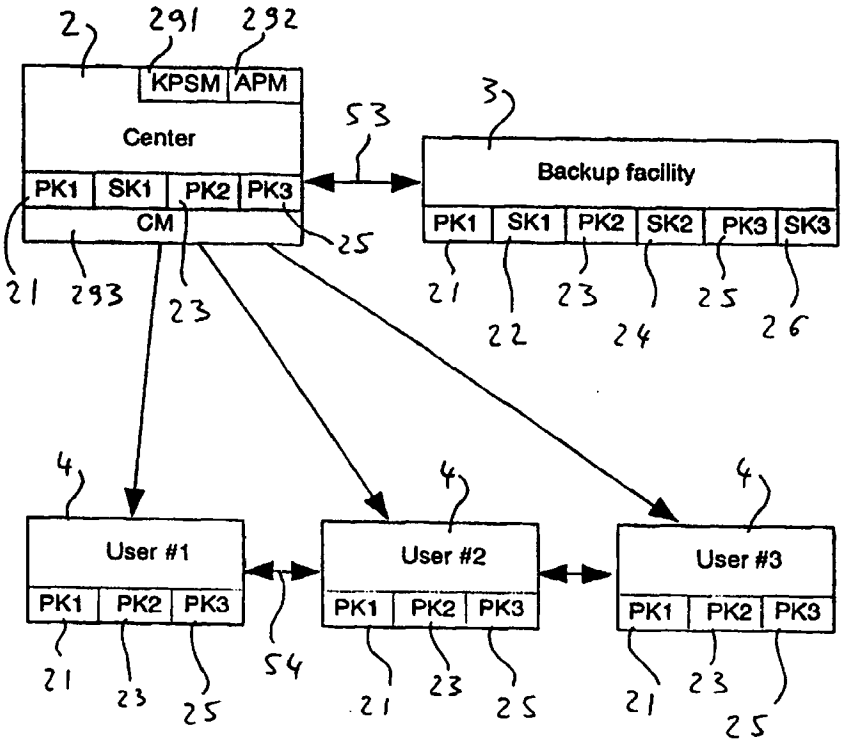
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SYSTEM AND METHOD FOR RELIABLE KEY TRANSFER

(57) Abstract

A system for reliable transfer of the center's keys to users, comprising: (A) a system for secure transfer of the encryption keys between parties (2, 4, 4, 4) located at separate locations; (B) means in the center for protecting the transactions using a public key method (21); (C) means for reliable key dissemination, comprising one or more additional key pairs at the center (23, 25); (D) means for generating or receiving a new key pair (291); (E) means for preparing announcements of a new public key for one of the key pairs (292). A method for reliable transfer of the center's key to users, comprising the steps of: (A) The center creates a new key pair (291); (B) a message is prepared at the center (292); (C) a plurality of secure messages are prepared from the message prepared in step (B); (D) the secure messages are collected into an announcement, which is sent to users.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

System and Method for Reliable Key Transfer

Technical Field

The invention concerns systems for reliable transfer of the encryption key and, in particular, to such systems which include means for recovery in case the private key of the center is compromised.

Background Art

Heretofore, various systems and methods were used to allow secure communications between parties located at locations separate from each other.
Secure communications involve the use of encryption, usually with a pair of public/private key. Throughout the present disclosure, the terms "private key" and "secret key" are used interchangeably, and are assumed to have the same meaning.

As global communications over the Internet or other means become more and more an essential element in business, science and all aspects of modern life, secure communications between remote parties gain in importance.

For parties located at separate locations from each other, there is the problem of secure transfer of the encryption keys. There is also the problem of authentication, that is for each party to a communication session to prove their identity to the other party.

Solutions to these problems in prior art involve the use of a center as intermediary between parties. The center either is involved in each transaction between parties, or issues "certificates", that is each party receives a data package attesting to their identity, encryption keys and related information, all encrypted or signed with the private (secret) key of the center. These applications use a "trusted center" .

Providers and users of these centers and certificates acknowledge that compromising the private key of the center is a "catastrophe" , that the result is a complete collapse of the system.
If the private key of the center is compromised, then nobody can trust nobody else. Neither the users nor the center can be trusted anymore.

Another field involving secure communications is between a center and users, for example between a software manufacturer and its customers.
The manufacturer may access the customers to send an update to a software package sold to that user, or a fix for a bug.
In either case, it is important that the user ensure the identity of the manufacturer. Otherwise, a malicious impostor may use the system to disseminate viruses, for example.

The authentication of the manufacturer and the reliability of the link may be based on a public/private key system.
Here, again, there is the question of the security of the manufacturer's private key. If that key is compromised, then the whole system collapses, and the manufacturer de facto loses contact with their customers.

It is a common assumption that the private key is very secure, and will take a very long time to break. That very long time, however, is a statistical result, the expected mean time; any single attempt, however, can succeed in breaking the key, since there is a finite nonzero probability for that, although the probability is low. It is possible that the key is compromised through bad luck or a a human error.

If the private key of the center was compromised, then it must be changed. This is required to achieve secure communications with users. It may be advantageous to change the center's private key on a regular basis, for example each year. This makes it more difficult to break that key and, in case the key is compromised, to limit the damage done.

One should take into acccunt that, once it is decided to change the keys of the center, the implementation may not be simple. One reason is that, if the key is compromised, then users cannot distinguish anymore between the center and an impostor.
An impostor may issue false certificates or otherwise act in ways detrimental to the center and/or the users.

The center cannot assert both that its key is compromised (therefore the center cannot be trusted anymore) and at the same time ask users to accept its new key, (thus asking users to trust the center, despite its compromised key).
The two statements are contradictory and, logically, do not allow a reliable change of the center's keys in the event they were compromised.

Thus, when the private key of the center is compromised, then a secure link with users cannot be established anymore, therefore a new key cannot be safely distributed. This is a vicious circle.

A method for encryption key dissemination to achieve a secure link between users at separate locations was disclosed in another application by the present inventor. The method is based on certificates issued by encryption key dissemination centers, with the centers being organized in a hierarchical, tree-like structure. Whereas the method supports encryption key dissemination between users who use the same hierarchical structure or tree, the method cannot be used between two users who each uses a different tree.

In a scenario where users are organized in separate groups, each group having its distinct hierarchy for certificate issuing centers, it may be desirable to have the capability to combine two tree structures into one, that is to allow the users of two separate trees to exchange certificates with each other. This would require a drastic change in the keys of the centers, which is difficult to implement.

It is an objective of the present invention to address the situation where the private key of the center was compromised or there are other reasons that demand a change of the center's encryption key pair.

Disclosure of Invention

It is an object of the present invention to provide a system and method for secure communications using a public/private key with means for recovery in case the private key of the center is compromised.
This object is achieved by means for recovery in case the private key of the center is compromised as disclosed in claim 1.

In accordance with the invention, the object is basically accomplished by providing means, located in the center and in the users' facilities, for secure dissemination of a new center's public key.

These means use not a single public/private key pair, but three key pairs. A first private key is stored in the center, with its corresponding public keys being stored in the center and also disseminated to all users.

The second and third private keys may be stored in a secure location related to the center, with their corresponding public keys being stored in the center and also with the users. Otherwise, all the keys may be stored in the center.

It is another object of the invention to achieve a system which is more secure and flexible than system that use a single encryption key pair.

The object is basically achieved with a method using a plurality of encryption key pairs. A first public/private key pair is used for daily activities, that is for communication between users and the center, and between users and themselves.
A second and a third key pairs are used to allow a secure replacement of any of the keys of the center. It is also possible to use these keys in lieu of the first key for data encryption.

A further object of the invention is to allow for effective and secure dissemination of a new center's key.

The object is achieved with a method for the dissemination of a new center's key, wherein the center issues "certificates" or "announcements" disclosing the new public key, and uses the second and third private keys to attest as to the authenticity of these "certificates" or "announcements" . Each user employs a majority check, that is a verification that the new key announcement is correctly attested by two known keys (the second and third key). Where there is a doubt regarding which key was changed, a majority check can clearly indicate that. For a majority check, a minimum of three key pairs should be used. If more than three key pairs are used, their number should be preferably odd.

Moreover, the announcement includes a declaration of each of the three keys, each backed by the other keys, that is a total of 6 announcements. This comprises the first stage of new key dissemination, including communications between the center and certain users.

Another object of the invention is to reduce the workload on the center which is required to send a message to each and every user in the system.

The object is achieved using a two-stage method, wherein during a first stage the center sends messages to part of the users, and a second stage wherein the message is communicated between users. In this second stage which includes communications between users and themselves, as each user with an updated certificate communicates with an user still holding the old certificate, the information relating to the new key of the center is transferred from the first user to the latter.

The method for a new key dissemination includes the three key pairs and adequate procedures in the center and at users' facilities, to enable automatic dissemination of the new key, supporting both the first and second stage of new a key. Thus, a secure, fast, efficient and easy dissemination of a new key is accomplished. User's intervention is not required.

The abovementioned system and method accomplish the secure dissemination of a new key for center, and thus achieve the recovery from the situation where the center's private key was compromised.

Moreover, the above system and method allow the center's key to be changed anytime there is doubt regarding the security of the key, or as a routine precautionary method, at predefined time intervals.

A method for encryption key dissemination is based on certificates issued by encryption key dissemination centers, with the centers being organized in a hierarchical, tree-like structure. A multiple-key method is disclosed that allows two separate trees to be combined into one structure to achieve overall certificate compatibility among users pertaining to the two separate trees.

Further objects, advantages and other features of the present inventionwill become obvious to those skilled in the art upon reading the disclosure set forth hereinafter.

Brief Description of Drawings

The invention will now be described by way of example and with reference to the accompanying drawings in which:

Fig. 1 details the structure of a system including means for secure dissemination of new key.

Fig. 2 illustrates the structure of an user certificate with new key announcement attached thereto.

Fig. 3 details the possible types of transactions between users, during the new key dissemination stage.

Modes for Carrying out the Invention

A preferred embodiment of the present invention will now be described by way of example and with reference to the accompanying drawings.

Fig. 1 details the structure of a system including means for secure dissemination of new key, including a center 2, the backup facility 3, and a plurality of users 4.

The system and method in the present invention use as a component therein a public key encryption method as known in the art. The public key method is based on an encryption key pair including a public key and a corresponding private (secret) key. Messages encrypted with the known public key can be decrypted with the secret key. Thus, although anyone can encrypt a message for a user X using their known public key, nobody can decrypt the message except that user X, since only user X holds the secret key corresponding to the public known key. The user X may be a user in the system or the key distribution center 2.

Center 2 normally uses a key pair comprising a secret key 22 and a corresponding public key 21. All the users in the system know the center's public key 21 and can send encrypted messages to center 2, with the messages being encrypted with public key 21.

Only center 2 can decrypt these messages, however, since only center 2 holds the secret key 22 corresponding to public key 21.

Similarly, center 2 can send to users messages encrypted with the secret key 22. This serves as a center's signature or authentication of the message, since any user can decrypt the message with the center's public key 21, however any user is aware that only center 2 could encrypt the message with their private key 22 so that it can be decrypted with key 21.

The above is a description of prior art methods using an encryption key pair in a public encryption scheme. The following description relates to novel aspects of the present invention, relating to the use of additional encryption key pairs (23, 24) , (25, 26) and of a backup facility 3.

It is advantageous to use three key pairs, since this allows the recipient to use a majority check to indicate which key was changed, according to methods to be detailed below.

In another embodiment, more than three keys may be used, in which case an odd number of keys should be used to allow a clear majority decision.

Although the following disclosure refers to a three key pair system, it is understood that the method and system in the present disclosure can be adapted for a larger number of key pairs, without departing from the scope and spirit of the present invention.

For a general case where N key pairs are used, the decision threshold is INT((N-1)/2). For example, if N= 6 then up to 2 keys in a message may be simultaneously in error.

The actual number of key pairs used may be decided by each organization, according to the desired level of safety/security, that is the number of keys it is expected may be simultaneously compromised. For example, if it is estimated that just a single key will be compromised, then three key pairs are enough. The other two keys are used in a majority vote to indicate a change in that key. If it is estimated that two keys may be compromised simultaneously, then a system with five key pairs should be used, so that the uncompromised three keys still will achieve a majority vote to allow the update of the two keys to be updated.

An advantage of the above method is its flexibility, which allows to achieve any desired level of security.

There is a backup link 53, between center 2 and backup facility 3, to allow use of the second secret key SK2 (24) and the third secret key SK3 (26) when a change of center's key is required. The method used in this case is disclosed below. Link 53 may be fixed or temporary, only to be established when necessary. For example, a telephone or wireless link is established when it is required to read a key from backup facility 3. In another embodiment, a storage means for the keys may be manually brought to the center 2, for example a diskette or a CD-ROM.

The backup facility 3 is optional. In another embodiment of the invention, all the keys are stored in center 2, using appropriate means to protect the private keys 22, 24 and 26.

Such protection means may include, for example, a storage means for the keys like a diskette or a CD-ROM. These storage means may be kept in a safe at center 2, to be safe and available when needed.

The novel system and method assumes that, although one private key may be compromised, the other private keys are secure and can be used for center recovery, as detailed below.

The above considerations relating to the protection of the private keys are applicable to the description of all key processing and transfer operations, throughout the present disclosure.

The center link 52, between center 2 and users 4, is used to issue certificates to users, as well as for the direct dissemination of a new key from center 2.

The users link 54, between users and themselves, is used for encrypted communications as well as for the exchange of certificates between users 4. The abovementioned links 52, 53, 54 may include digital communication links as known in the art, including but not limited to telephone lines, the Internet, local area nets, wireless links or a combination thereof.

There are several encryption keys at center 2, as follows:

A. a first public key 21, used for regular work at center, as required;
B. a first secret key 22, used to prepare encrypted certificates which are issued to users 4.

C. a second public key 23 and third public key 25, used for a new key dissemination only, according to the methods disclosed below.

All the keys used in the system may be stored at a backup facility 3: the first public key 21, first secret key 22, second public key 23 and third public key 25 are identical to the corresponding keys at center 2.

The second secret key 24 and the third secret key 26 are used for the dissemination of a new key, when a new key pair is generated at center 2. It is also possible to use second and third private keys 24, 26 to sign or encrypt messages or certificate, as decided by the system operator. The keys may be used interchangeably, if it was decided to do so.

It is possible to store all the keys at center 2. In a preferred embodiment of the present invention, however, a method is disclosed where the keys used to facilitate the dissemination of a new center key are stored at a separate location. This is preferred since, should there be a factor to compromise the first secret key SK1 (22) at center 2, the other secret keys will remain protected because of their separate location.

The keys stored at each user's facility 4 include:
A. a first public key 21, is used for regular communication with center 2 and other users 4;
B. a second public key 23 and third public key 25, are used for receiving a new key from center 2.

Actually, each of the keys 21, 23 or 25 at the user's facility can be updated according to the present invention, based on the other two keys. The user receives an announcement regarding a change in one of the keys 21, 23, 25 , signed by the other two keys. This is a solid base to accept the new key announcement and update the storage accordingly.

Thus, means are included, in the center and in the users' facilities, for secure replacement of the communication keys with the center.

In the exemplified embodiment as presented, there are three key pairs (21, 22) , (23, 24) and (25,26).
Other embodiments include a different number of key pairs, preferably an odd number. An odd number is useful to reach a correct decision when more than one key is compromised or changed, or some of the data becomes corrupted. For a general case where N key pairs are used, the decision threshold is INT((N-1)/2).

Center 2 further includes means 291 (Key Pair Setting Means KPSM) for setting up a new key pair at the center 2. Means 29 may include means for generating a new key pair, or means for receiving a new key pair from another location, using secure communication means. In any case, the new key pair thus set up will comprise a new private key and a new public key for the center 2.

Center 2 includes means 292 for preparing an announcement of a new public key for center 2, the Announcement Preparation Means (APM).

The announcement includes one or more copies of a message disclosing the new public key. The number of copies of the message equals the number of additional key pairs for reliable key dissemination, and each copy of the message is encrypted or signed with the private key of one or more of the additional key pairs.

Furthermore, center 2 includes communication means 293 (CM) for transferring the announcements to users 4 in the system. The announcement may include the new public key together with additional optional information as detailed in the present disclosure.

A method for changing a key pair at center 2 will now be detailed with reference to Fig. 1.

Method 1 – Changing the key at center 2

A. The Key Pair Setting Means 291 (KPSM) at center 2 is activated to set up a new key pair. Thus center 2 creates a new key pair for the key to be changed. For example, if the first key is to be changed, then the new key pair would include a new public key PK1' and a new private (secret) key SK1' . Otherwise, a key pair may be independently generated and sent to the center;

B. the new key pair (PK1' SK1') is optionally stored at the backup facility 3;

C. the Announcement Preparation Means (APM) 292 at center 2 is activated to prepare an announcement or message announcing that the first public key was changed, and the new value for the first public key PK1'. In general, the message includes an indication as to which key pair was changed, and the new value of the public key for that key pair;

D. a plurality of secure messages are prepared from the message prepared in step (C), wherein each secure message is prepared by a procedure of encryption or a digital signature of said message with one of the secret keys SK2, SK3 pertaining to said key pairs in the center. In one embodiment, a secure message is prepared, where the message prepared in step (C) is encrypted with each of the secret keys SK2, SK3, to create two versions of the message.

In another embodiment, the message may be left unchanged, and made secure with digital signatures which are prepared and added to the message. Each signature includes a hash of the message, encrypted with one of the private keys;

E. the secure messages or message with digital signatures are collected into a new key announcement, which is sent to users 4 using the communication means 293 (CM) located at center 2.

F. users 4 each decrypts the announcement, where in the present example the two message decrypt OK since the known key was used;

G. since two independent copies of the message, that is copies that were signed with two independent keys, decrypt OK, the user 4 accepts the message as true and updates their records with the new value of the first public key PK1' for center 2.
End of method.

Thus, the second and third key pairs are used to allow a secure replacement of the first key pair at the center. Accordingly, any two keys can be used to perform a change in the third key.

The center 2 issues "announcements" disclosing the new public key, and uses the private keys to attest as to the authenticity of these "announcements" . Each user 4 employs a majority check, that is a verification that the new key announcement is correctly attested by two of the known keys of center 2.

Although the above example illustrates the method for changing the first key pair at center 2 and announcing that to users 4, it is to be understood that the same method can be also used to change other key pairs at center 2. In any case, two copies of the message will decrypt OK and will be identical to each other, thus reliably indicating a change in the third key (that is, the chance that two independent messages using different keys will give identical results for the third key is practically zero, unless the two messages indicate a true change of the third key).
Thus, the three key system and method allow to securely transfer the information regarding an encryption key change to users 4.

A multiple key change method

The present invention is not limited to the change of just one key pair at a time; several key pairs may be changed simultaneously. The method may be used when all the keys are believed secure, and there are other reasons to perform that key update.

The method comprises the following steps:

A. The Key Pair Setting Means 291 (KPSM) at center 2 is activated to set up a plurality of new key pairs. Thus, center 2 creates new key pairs for the keys to be changed. For example, three key pairs are generated in a three key system to simultaneously replace all the keys there.

B. the new key pairs are optionally stored at the backup facility 3;

C. the Announcement Preparation Means (APM) 292 at center 2 is activated to prepare an announcement or message announcing that the public keys were changed, and the new value for the public keys PK1' , PK2 etc. In general, the message includes an indication as to which key pairs were changed, and the new value of the public keys for each key pair. Alternately, a message may include a list of all the public keys after the changes performed.

D. a plurality of secure messages are prepared from the message prepared in step (C), wherein each secure message is prepared by a

procedure of encryption or a digital signature of said message with one of the secret keys SK1, SK2, SK3 etc. pertaining to said key pairs in the center. An encryption with the old secret keys is performed, that is using the keys as used before step (A) above, the keys known to users in the system.

E. the secure messages or message with digital signatures are collected into a new key announcement, which is sent to users 4 using the communication means 293 (CM) located at center 2.

F. users 4 each decrypts the announcement using the known decryption keys, where in the present example all the message decrypt OK since the known keys were used;

G. since several independent copies of the message, that is copies that were signed with independent keys, decrypt OK, the user 4 accepts the message as true and updates their records with the new value of the public keys for center 2.
End of method.

A hash signature method

In another embodiment of the invention, in step (D) the message is not encrypted, but signed with the private keys of center 2. A digital signature includes the computation of a hash, or a group of bytes from the message.

That hash is then encrypted with the private key as desired, and attached to the message. Thus, anyone can read the message, and can later, if necessary, verify its reliability by computing a hash and comparing with the signature, after the signature is decrypted using the public key.

Throughout the present disclosure, where encryption is used to attest as to the truth of a message, the above hash signature method may be used in lieu of the encryption.

In a preferred embodiment, the message prepared in step (D) in Method 1 includes:

1. the first public key of center 2
2. the second public key
3. the third public key
4. a hash of items (1+2+3) above, encrypted with the first private key of center 2
5. a hash of items (1+2+3) above, encrypted with the second private key of center 2
6. a hash of items (1+2+3) above, encrypted with the third private key of center 2 .

Alternately, items 4, 5 and 6 may include each the items (1+2+3) above, encrypted with the appropriate private key.

The above message forms a certificate indicating the updated public keys of center 2, to be disseminated to users.

A user, upon receiving the above certificate, decrypts with each of the known public keys of center 2, to verify the signatures for the message. Each message or hash that compares OK is tagged as such. If the number of signatures that are OK exceeds a threshold (2 out of 3, for example), then the message in the certificate is accepted by the user as valid, and the keys therein are used to indicate the updated keys for center 2.

If the key of the center was changed, it may be necessary for users to change their certificates, so as to be encrypted with the new key of the center. The three key system and method can be used to reliably notify the users in the system that the center encryption key was changed, so that a certificate update may be necessary.

Such a notification may be impossible to send in prior art systems, where the compromise of the center's key is considered a complete disaster. After such a disaster the center cannot be trusted anymore, so its notices may not be accepted by users. Moreover, in existing systems the center should contact each and every user to try to notify them, a very difficult task in a worldwide network with millions of users.

Thus, the present invention provides secure means for communicating between a key distribution center and users in the system, even when a center's key becomes compromised. These secure communication means may be advantageously used to disseminate a new key to users and to allow the update of user's certificates.

In still another embodiment of the invention, in step (D) there are created six messages, which include statements regarding all the public keys of center 2, each endorsed with the private keys of the other pairs.

Thus, the messages in the announcement are (for a three key embodiment):

Message #1= Sk2 (Center ID, Pu1)

Message #2= Sk3 (Center ID, Pu1)

Message #3= Sk1 (Center ID, Pu2)

Message #4= Sk3 (Center ID, Pu2)

Message #5= Sk1 (Center ID, Pu3)

Message #6= Sk2 (Center ID, Pu3)

Thus, Message #1 includes information identifying the center 2, with the public key #1, all encrypted with the secret key #2.

Message #2 includes information identifying the center 2, with the public key #1, all encrypted with the secret key #3. The same method is applied on a circularly cyclic order, to the other keys.

If there are more than three key pairs, then there are more than six messages, using the same method. Similar methods will become apparent as well.

Each user, upon receiving these or similar messages, will try to decrypt them all with the known keys. A majority vote decision may be implemented, with the unchanged keys being used to attest to the changed key. Thus, the message relating to the key change will be accepted by the users.

An announcement from center 2 may include either information on the key which was changed, or a declaration as to the valid keys at the center at present. In the former case, the users change the key accordingly. In the latter case, the users compare the key values at center with the keys at the user facility, and update what is necessary.

The messages may include a signature with the corresponding keys, in lieu of the encryption, as follows:

Message #1= Center ID, Pu1, Sk2 (Hash (Center ID, Pu1))
Message #2= Center ID, Pu1, Sk3 (Hash (Center ID, Pu1))
Message #3= Center ID, Pu2, Sk1 (Hash (Center ID, Pu2))
Message #4= Center ID, Pu2, Sk3 (Hash (Center ID, Pu2))
Message #5= Center ID, Pu3, Sk1 (Hash (Center ID, Pu3))
Message #6= Center ID, Pu3, Sk2 (Hash (Center ID, Pu3))

Thus, for example, Message #1 includes the Center identification and the public key #1 without encryption, and also a digital signature comprising a hash of the above message, with the hash being encrypted with the private key #2. Similarly, message #2 includes the Center identification and the public key #1 without encryption, and also a digital signature comprising a hash of the above message, with the hash being encrypted with the private key #3.
Thus, the public key #1 is attested to with the other two keys at the center. Similarly, the Messages #3 to #6 are used to attest for the public keys #2 and #3, each with the remaining two keys.

In another embodiment of the invention, only two announcements are included, with signatures using each of the unchanged keys:

Message #1= Center ID, Pu1, Sk2 (Hash (Center ID, Pu1))
Message #2= Center ID, Pu1, Sk3 (Hash (Center ID, Pu1))

Thus, the announcement regarding the new value of key #1 is attested by the signature with key #2 and #3 each on the hash of the announcement. The rational for this implementation is that the three presently used keys are known to all the users, and there is no real need to again disseminate them. Only the messages relating to a new key bring real information to users (something which is not known as yet) and justify a message dissemination process.

In still another embodiment of the invention, only one announcement is included, with attached signatures using each of the keys:

Message #1= Center ID, Pu1, Sk2 (Hash (Center ID, Pu1)),
Sk3 (Hash (Center ID, Pu1))

Thus, the announcement regarding the new value of key #1 is attested by the signature with key #2 and #3 each on the hash of the announcement.

The use of signatures allows a faster, more efficient of the message at the user's facility. Thus, when an announcement is received, then the keys information is evaluated, to check whether a key was changed.

If not, there is no need for further processing. If the announcement indicates that a key was changed, then the signature is processed (decrypted) to ensure the announcement is legitimate.

It may be necessary for the center to change a second key only a short time after the first key was changed, that is before the change of the first key was updated with all the users. To cope with such a situation, each announcement of a key change may include the issue date or a serial number. Each user, when receiving more than one announcement of a key change from center, will arrange these announcements in their order of issuance and will perform the key change in the required order.

The above method allows to securely convey information regarding a new key to users, however a large effort on the part of center 2 is required, since center 2 has to contact all the users of that system. A typical system may include millions of users, widely dispersed, possibly on a worldwide scale. Thus, direct key transfer from center 2 to each and every user 4 may be difficult.

This problem is addressed in the present invention with the disclosure of an automatic method for spreading the information on a new key directly between users 4 , after the process is initiated by center 2.

Thus, the abovedetailed announcements from center to users comprise just the first stage of a two-stage key dissemination method, herein disclosed.

Fig. 2 illustrates a new, two-stage method, wherein a new type of user certificate is used. The certificate or announcement 7 includes three copies of a message regarding the key which was changed, each message being signed or encrypted with one of the private keys of the center:

Message 71 encrypted with the first private key ;
Message 72 encrypted with the second private key ;
Message 73 encrypted with the third private key .

Note: Although all the possible messages 71, 72 and 73 were illustrated for clarity, it is only necessary to include two messages in the announcement, that is the messages encrypted or signed with the unchanged private keys.

In another embodiment of the invention, a certificate includes statements regarding each of the public keys at the center 2, where for each key the statement is signed with the private key of the other pairs. For three key pairs, there would be 6 copies of the message, as detailed above.

The certificate may be distributed as a routine, all the time, or following a key change at the center. The center 2 issues certificates 6 with new key announcement 7 attached thereto.
Center 2 issues the above announcements regarding the new key pair to only part of the users 4, preferably a small part of all the users' population.

The above is the first stage of a new key dissemination method.

The second stage invoives direct communications between users 4, wherein the new center key is transferred between users and themselves. Since the number of direct transactions between users is so much larger than the number of transactions with the center, the second stage will accomplish the bulk of the new key dissemination workload, without requiring center's intervention. Thus, there is no danger that the center may collapse or be overworked during the new key distribution.

One should take into account that the user's certificates have to be updated, and therefore a certain effort on the part of the center 2 will be required. This, however, can be performed in a secure way, and the workload can be distributed among the various centers in a network.

Following is a disclosure of examples of methods which can be used for the new key dissemination using the two-stage method, and with a plurality of key pairs, of which one pair is used for regular communications and the other key pairs are used for key changes.

Method 2 – Preparation of an announcement for a new key J

A. Prepare message including: the new public key J, an indication that a key was changed and as to which of the N key pairs was changed (that is, key J) and optional additional information;

B. compose the announcement, to include N copies of the message in step (A) above, wherein N is the number of key pairs, each copy including the above message, encrypted with one of the private key of the N key pairs.
For the key pair J which was changed, use the new secret key J for encryption;

C. attach the above announcement to the new certificate being sent to each user.
End of method.

Method 3 – Handling of a new key announcement by recipients/users

A. Recipient will decrypt all the copies of the message, each with its corresponding public key. All the copies will decrypt OK, except that encrypted with the new key J, which is unknown as yet to recipient;

B. recipient will compare the decrypted messages, and conclude that the majority thereof tally OK. For three keys, there will be two messages which decrypt OK, that is those with the keys which remain unchanged;

C. since two out of three messages were decrypted and are identical, then recipient accepts the message as true.
In that case, the contents of the message is interpreted and acted on, that is the recipient accepts a new tentative value for the new public key J;

D. recipient now tries again to decrypt copy J of the announcement (the copy which did not decrypt because the old key J was used), this time using the new tentative public key J as received;

E. if the result is OK, that is the decryption was successful and the decrypted copy is identical to the other copies decrypted in stage (A) above, then new public key J is accepted as true, and the records at recipient are updated with the new public key J;

F. (optional) if the result is not OK, then sender is notified that the announcement is not acceptable.
End of method.

Variations of the above methods:

1. The method allows for periodical change of all keys, for example on a rotary basis. This preserves the security of the system, since a small effort at prevention may greatly increase the difficulty of breaking the key of the center.

2. any numbers of keys can be used, preferably an odd number. Then any of the keys can be changed anytime at center's discretion, using an announcement signed by the other keys. The announcement includes several copies of the key change message, each signed (encrypted with the private key) of one of the other key pairs.

A user/recipient will decrypt these messages, and will compare them . If N out of M messages tally up (are identical) with M the total messages and N a predefined threshold, for example M/2, then the request for key change will be honored, otherwise the request will be rejected.

Thus, the abovedetailed methods enable automatic dissemination of the new key, supporting both the first and second stage of new a key. Thus, a secure, fast, efficient and easy dissemination of a new key is accomplished. User's intervention is not required.

By providing for the secure dissemination of a new center's key, the novel methods in the present invention can be used to perform a recovery from a situation where the center's private key was compromised.

Moreover, the above system and method allow the center's key to be changed anytime there is doubt regarding the security of the key, or as a routine precautionary method, at predefined time intervals or as decided. Thus, a flexible and powerful private key protection scheme is implemented using the system and method in the present disclosure.

A method for combining key dissemination trees

A method for encryption key dissemination is based on certificates issued by encryption key dissemination centers, with the centers being organized in a hierarchical, tree-like structure.

A multiple-key method is disclosed that allows two separate trees to be combined into one structure to achieve overall certificate compatibility among users pertaining to the two separate trees. In one embodiment of the invention, the center of a first tree is updated to be compatible with the center of a second tree.

The method comprises the following steps:

A. Both certificate issuing hierarchies or trees have a multiple-key structure as detailed above For example, each key issuing center has three key pairs. The users in each tree know the public keys for all the key pairs there.

B. The keys in the highest level center of the first tree are changed, to the values of the corresponding keys in the center of the second tree. For example, in a three key pair system, the first public key PKA1 is changed to the value of the first key PKB1 in the other tree, the second public key PKA2 is changed to the value of PKB2, and PKA3 is changed to PKB3. The change may be implemented as detailed above, in the method for simultaneous change of several keys.

C. The highest level center in the first tree issues certificates to the centers one level lower in the hierarchy, including the information relating to the new keys.
End of method.

The result of the above method is that now users in the two trees can exchange encryption keys with each other, since the two trees are based on public keys that are identical at the highest level. This is equivalent to a situation where the two separate centers are replaced with one common center at the highest level, so that the two separate trees become one united tree.

The above method may be advantageously used when two firms or networks unite and there is a need to achieve compatibility and interoperability among all the users of the two original firms or networks.

In another embodiment of the method, the two highest level centers in the two trees are replaced with a third center which is to replace the two centers in the united tree. The new center is issued several new key pairs, which are to be used throughout the new united tree.
The centers in the next level (one level below the highest) are issued certificates indicating the new public keys of the new center. The result is that the new center effectively replaces the two existing centers, and the common center unites the two trees into one combined structure.

Fig. 3 details the possible types of transactions between users, during the second stage of the new key dissemination process. The diffusion of the new key information among users is mainly random, as users contact each other for their own purposes to perform desired transactions therebetween, without a prior knowledge of the most up-to-date information regarding the keys at center 2.

Part of the initial transaction between users is an exchange of certificates from center 2, that is certificates including key update information as prepared in Step (D) of Method 1 above. The exchange between users results in a transfer of the information regarding the new key for center 2, as detailed below.

There are two types of users: Each user may be initiated, that is having the new key of the center, or uninitiated, that is having the old key.
There are also two parties to a communication session: the caller and the respondent.

Thus, in all there are four types of transactions as illustrated in Fig. 3:

1. Uninitiated caller – Uninitiated respondent
2. Initiated caller – Uninitiated respondent
3. Uninitiated caller – Initiated respondent
4. Initiated caller – Initiated respondent

For each of the four possible types of transactions, the following corresponding method details an example of handling the initiation stage of the communication session to allow dissemination of the new center's key.

Method 4 – Type 1 transaction

The following transaction occurs between an uninitiated caller and an uninitiated respondent:

A. Caller identifies itself with the old certificate, using old center's key;

B. Respondent identifies itself in return, secure link is established.
The users perform a communication session, without being aware that the key may be compromised and is in the stage of being replaced.
End of method.

Both users, prior to the present transaction, had no contact with the center after a new key was introduced there, and no contact with an initiated user. This type of transaction is temporary, until the news of the new key spread to at least one of these users. Then a different transaction will take place, as detailed in Methods 2 to 4 below.

Method 5 – Type 2 transaction

The following transaction occurs between an initiated caller and an uninitiated respondent:

A. Caller identifies itself with the new certificate, using new center key;

B. Respondent cannot read the certificate presented by caller, since they use the old key;

C. Respondent reads the announcement attached to certificate from caller, decrypts the first part of the message therein using PK2, and also decrypts the second part of the message using PK3. If the messages are identical, then new key PK1' is accepted as true, and the records at respondent are updated accordingly. Continue (jump to) either step (D) or (E) below, since there are two possible continuations of the method;

D. Respondent continues present transaction using new key for center. It decrypts certificate from caller, answers, establishes link. END.
This step may be used if caller and respondent consider this not a high security session. The certificate may not be updated because the key was changed.

or:

E. Respondent connects center, using new public key PK1' , and asks for new certificate, encrypted with new private key SK1' . Center sends the certificate, together with announcement attached;

F. Respondent connects the previous caller, can identify itself with new certificate and perform secure session, Type 4 as detailed below.
End of method.

Result: news of new center's key was transferred to another user. Any user contacted by an initiated user will update their records, with the new center's key, and will ask new certificate for themselves.

Method 6 – Type 3 transaction

The following transaction occurs between an uninitiated caller and an initiated respondent:

A. Caller identifies itself with the old certificate, using old center's key;

B. Respondent cannot decrypt the certificate with the new center's key PK1' . Respondent recognizes the certificate uses the old key, and notifies the caller accordingly. Respondent sends its new certificate, with the announcement regarding the new center's key.

C. Caller reads the announcement attached to certificate from respondent, decrypts the first part of the message therein using PK2, and also decrypts the second part of the message using PK3.

If the messages are identical, then new key PK1' is accepted as true, and the records at caller are updated accordingly.

Continue (jump to) either step (D) or (E) below, since there are two possible continuations of the method;

D. Caller continues present transaction using new key for center. It decrypts certificate from respondent, answers, establishes link. END.
This step may be used if caller and respondent consider this not a high security session. or:

E. Caller connects center, using new public key PK1' , and asks for new certificate, encrypted with new private key SK1' . Center sends the certificate, together with announcement attached;

F. Caller connects again the previous recipient, can identify itself with new certificate and perform secure session, Type 4 as detailed below. End of method.

Method 7 – Type 4 transaction

The following transaction occurs between an initiated caller and an initiated respondent:

A. Caller identifies itself with the new certificate, using new center key;

B. Respondent decrypts the certificate with the new center's key PK1' . Respondent recognizes and accepts the certificate thus presented;

C. Respondent sends its own new certificate, to establish their identity. Thus respondent identifies itself in return, and a secure link is established.

No key update is necessary at either party; both have the new key, which was acquired independently by each party;

D. The users perform a secure communication session, with the new center key and new certificates.
End of method.

Various embodiments of the system and method pertaining to the present disclosure are possible, without departing from the scope and spirit of the invention.

For example, in the above embodiment there are three key pairs.
It may be possible to use only two key pairs, with only two new key announcement. In that case, each announcement relates to one public key, signed or encrypted with the private of the second key.

In this case, however, if there is disagreement between the two announcements, the user could not decide which announcement to accept as true.

Thus, it appears that three keys is a minimal practical embodiment.
Three keys allow the user to decide which statement to believe, based on a majority vote method – if two announcements present the same key, then they are true.

Other embodiments may include a larger number of key pairs, that is 4, 5 or more.

Preferably an odd number of key pairs should be used, so that a majority vote will always render a definite value.
Any key at center may be changed as often as desired. An announcement is sent to user, where two keys attest for the correctness of the third.

It will be recognized that the foregoing is but one example of an apparatus and method within the scope of the present invention and that various modifications will occur to those skilled in the art upon reading the disclosure set forth hereinbefore.

Claims

1. In a system using a center for secure distribution of encryption keys, certificates and/or permits to users located at separate locations using a public/private key pair, means for changing the encryption key pair comprising:

(A) means for storing the encryption key pair together with two or more additional encryption key pairs;

(B) means for setting up a new key pair that comprises a new private key and a corresponding public key for said center;

(C) means for preparing an announcement of said new public key for said center, wherein said announcement includes one or more copies of a message disclosing said new public key, with the number of said message equals the number of additional key pairs for reliable key dissemination, and each copy of said message is encrypted or signed with the private key of one or more of said additional key pairs; and

(D) communication means for transferring said announcement, including said new public key, to said parties or to others who communicate with said center.

2. The means for changing the encryption key pair according to claim 1, wherein users and parties to the secure distribution of encryption keys, certificates and/or permits further include means for storing the public keys for the additional key pairs.

3. The means for recovery in case the private key of the center is compromised according to claim 1, wherein said center is either involved in each transaction between said parties or issues certificates attesting to the public key of each of said parties.

4. The means for recovery in case the private key of the center is compromised according to claim 3, wherein said center further includes means for protecting said transactions and/or said certificates using a public key encryption method, wherein said method uses a public/private key pair with the public key known to said parties and the private key known only to said center.

5. A system for reliable transfer of the center's key to users, comprising:

(A) a system for secure transfer of the encryption keys between parties located at separate locations, including a center which is either involved in each transaction between said parties or issues certificates attesting to the public key of each of said parties;

(B) means in said center for protecting said transactions and/or said certificates using a public key encryption method, wherein said method uses a public/private key pair with the public key known to said parties and the private key known only to said center;

(C) means for reliable key dissemination, comprising one or more additional key pairs at said center, with the public keys corresponding to said key pairs being known to said parties;

(D) means for generating or receiving a new key pair, comprising a new private key and a new public key, to replace any of said key pairs at said center; and

(E) means at said center for preparing announcements of a new public key for one of said key pairs, wherein said announcement includes one or more copies of a message disclosing said new public key, wherein the number of said message equals the number of additional key pairs for reliable key dissemination, and each copy of said message is encrypted or signed with the private key of one of said key pairs.

6. The system for reliable transfer of the center's key to users according to claim 5, wherein the messages in the announcement relating to the new public key for one key pair are encrypted with all the private keys pertaining to all the key pairs, except the key corresponding to the pair which was changed and is being disclosed in said announcement.

7. A method for reliable transfer of the center's key to users, wherein said center stores a plurality of encryption key pairs, comprising the steps of:

(A) The center creates one or several new key pairs for the keys to be changed;

(B) a message is prepared at the center, announcing the updated public keys;

(C) a plurality of secure messages are prepared from the message prepared in step (B), wherein each secure message is prepared by a procedure of a digital signature or encryption of said message with one of the secret keys pertaining to said key pairs in the center; and

(D) the secure messages are collected into a new key announcement, which is made available to users.

8. The method for reliable transfer of the center's key to users according to claim 7, wherein the public keys corresponding to said key pairs at center are made available to user prior to said new key generation and dissemination.

9. The method for reliable transfer of the center's key to users according to claim 7, wherein said center includes a key pair for regular use and two additional key pairs used during a new key dissemination process, and wherein in step (C) there are prepared six secure messages or six digital signatures, each using one of the key pairs which was not changed.

10. The method for reliable transfer of the center's key to users according to claim 7, wherein said message in step (B) further including data to identify said center.

11. The method for reliable transfer of the center's key to users according to claim 7, wherein said secret keys are stored in a backup facility.

12. The method for reliable transfer of the center's key to users according to claim 7, wherein in step (A) all the key pairs are set to values corresponding to the keys in a second center and wherein the method is used to combine the users of the center with the users of the second center so as to achieve compatibility between all the users.

13. A method for reliable transfer of the center's key to users, wherein said center stores a plurality of encryption key pairs, comprising the steps of:

(A) Said center creates one or more new key pairs for the keys to be changed;

(B) a message is prepared at the center, including the updated values of the public keys in the center;

(C) a hash of the message prepared in step (B) is computed;

(D) a plurality of signatures are prepared from the hash computed in step (C), wherein each signature is prepared by a procedure of encryption of said hash with one of the secret keys pertaining to said key pairs in the center: and

(E) the message prepared in step (B) and the signatures prepared in step (D) are collected into a new key announcement, which is made available to users.

14. The method for reliable transfer of the center's key to users according to claim 13, wherein in step (D) the encryption is performed with the secret keys prior to the keys update.

15. The method for reliable transfer of the center's key to users according to claim 13, wherein in step (A) all the key pairs are set to values corresponding to the keys in a second center and wherein the method is used to combine the users of the center with the users of the second center so as to achieve compatibility between all the users.

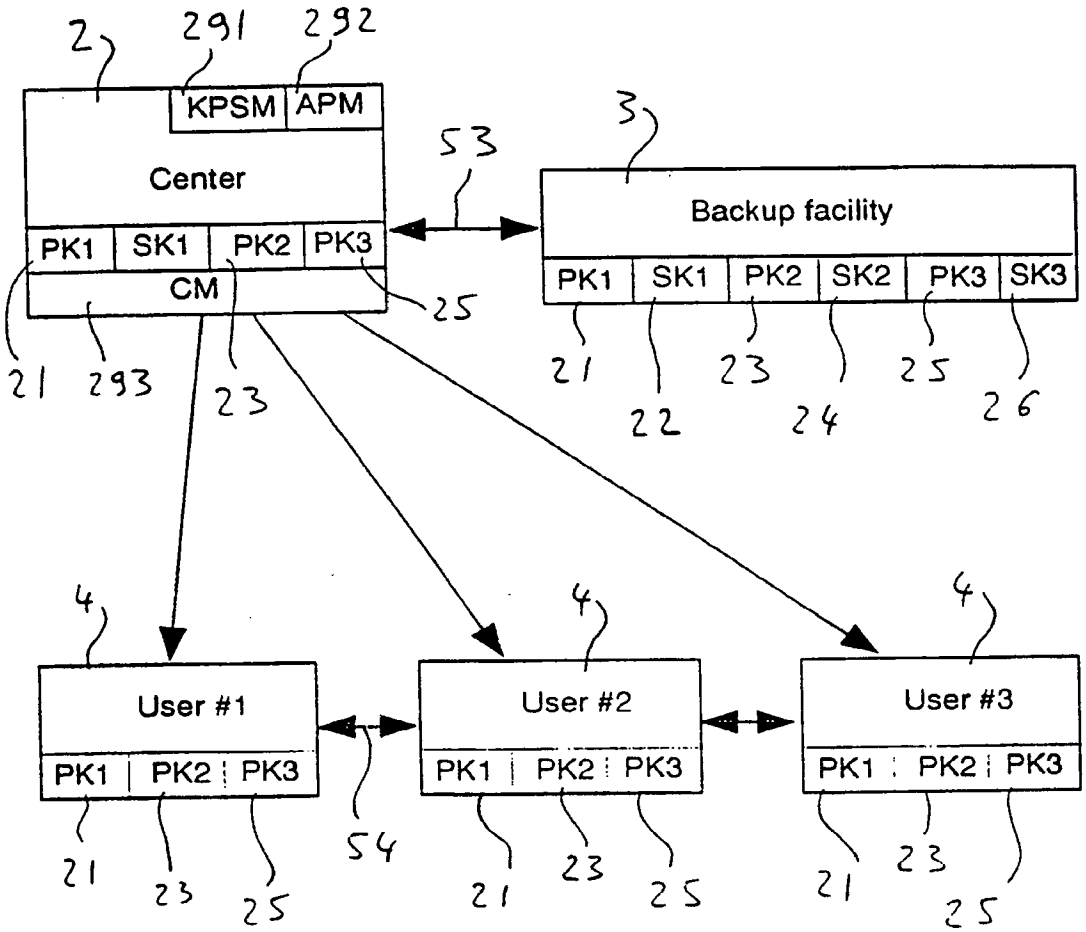

2
291
292
KPSM
APM
Center
PK1
SK1
PK2
PK3
CM
53
3
Backup facility
PK1
SK1
PK2
SK2
PK3
SK3
25
21
293
23
21
22
23
24
25
26
4
User #1
PK1
PK2
PK3
54
4
User #2
PK1
PK2
PK3
4
User #3
PK1
PK2
PK3
21
23
25
21
23
25
21
23
25

Fig. 1

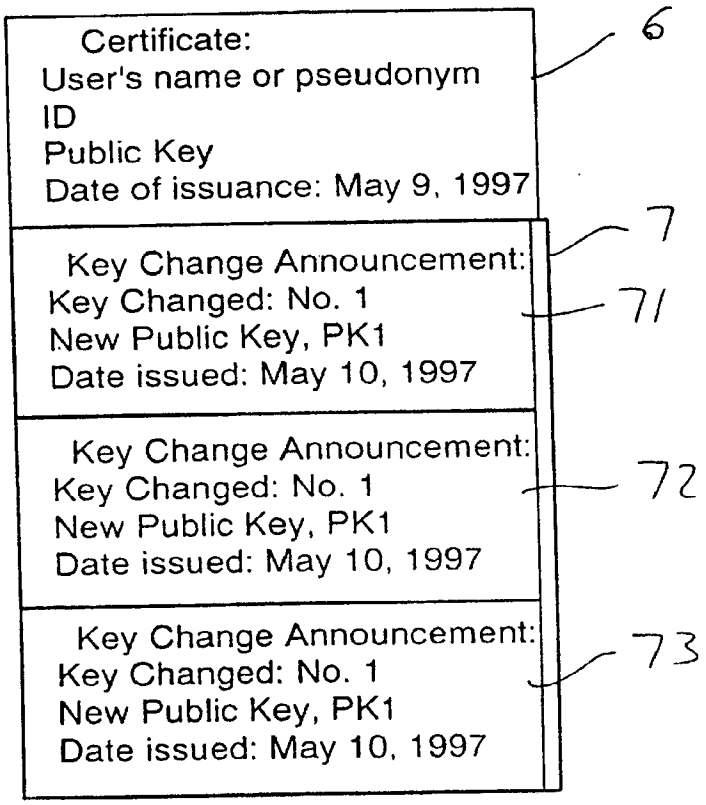

Certificate:
User's name or pseudonym
ID
Public Key
Date of issuance: May 9, 1997
6
Key Change Announcement:
Key Changed: No. 1
New Public Key, PK1
Date issued: May 10, 1997
7
71
Key Change Announcement:
Key Changed: No. 1
New Public Key, PK1
Date issued: May 10, 1997
72
Key Change Announcement:
Key Changed: No. 1
New Public Key, PK1
Date issued: May 10, 1997
73

Fig. 2

Caller / Respondent	Uninitiated	Initiated
Uninitiated	Transaction Type 1	Transaction Type 2
Initiated	Transaction Type 3	Transaction Type 4

Fig. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IL98/00381

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/08, 9/16, 9/30
US CL :38303/21, 25, 49

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/21, 25, 49

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS: key distribution center; key exchange; key(2a)change; plural(2a)signature#

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, P	US 5,680,458 A (SPELMAN et al) 21 October 1997, see column 2, lines 29-43.	1-15
A, P	US 5,761,306 A (LEWIS) 02 June 1998, see column 10, lines 17-25.	1-15
A	US 5,404,403 A (BRIGHT et al) 04 April 1995, see column 2, lines 17-25.	1-15
A	US 5,081,677 A (GREEN et al) 14 January 1992, see column 8, lines 33-49.	1-15

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 16 NOVEMBER 1998	Date of mailing of the international search report 14 JAN 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer GILBERTO BARRÓN JR. Joni Hill Telephone No. (703) 305-1830

Form PCT/ISA/210 (second sheet)(July 1992)★